国家互联网应急中心

网络安全信息与动态周报

2021 年第 3 期

1 月 11 日-1 月 17 日

CNCERT/CC

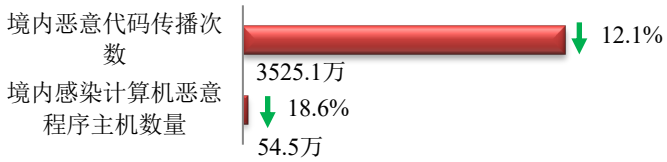
本周网络安全基本态势

境内计算机恶意程序传播次数 境内感染计算机恶意程序主机数量	•3525.1万 •54.5万	↓12.1% ↓18.6%
境内被篡改网站总数 其中政府网站数量	•3657 •23	↑14.0% ↓4.2%
境内被植入后门网站总数 其中政府网站数量	•772 •3	↓48.0% ↓86.4%
针对境内网站的仿冒页面数量	•1742	↓58.4%
新增信息安全漏洞数量 其中高危漏洞数量	•566 •224	↑111.2% ↑148.9%

表示数量与上周相同 *表示数量较上周环比增加* *表示数量较上周环比减少*

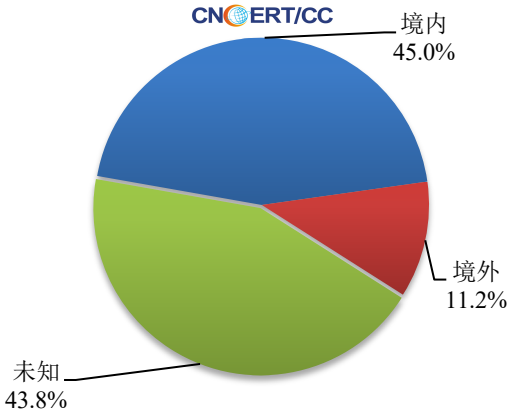
本周网络病毒活动情况

境内计算机恶意程序传播次数约为 3525.1 万次，境内感染计算机恶意程序主机数量约为 54.5 万个。

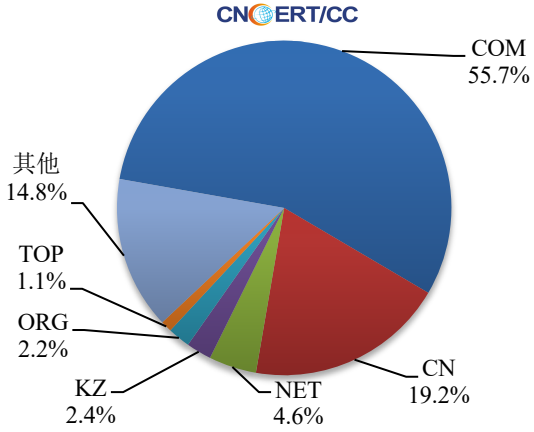


放马站点是网络病毒传播的源头。本周，CNCERT 监测发现的放马站点共涉及域名 738 个，涉及 IP 地址 8269 个。在 738 个域名中，有 11.2%为境外注册，且顶级域为.com 的约占 55.7%；在 8269 个 IP 中，有约 14.0%位于境外。根据对放马 URL 的分析发现，大部分放马站点是通过域名访问，而通过 IP 直接访问的涉及 565 个 IP。

本周放马站点域名注册所属境内外分布
(1/11-1/17)



本周放马站点域名注册所属顶级域分布
(1/11-1/17)



针对 CNCERT 自主监测发现以及各单位报送数据，CNCERT 积极协调域名注册机构等进行处理，同时通过 ANVA 在其官方网站上发布恶意地址黑名单。

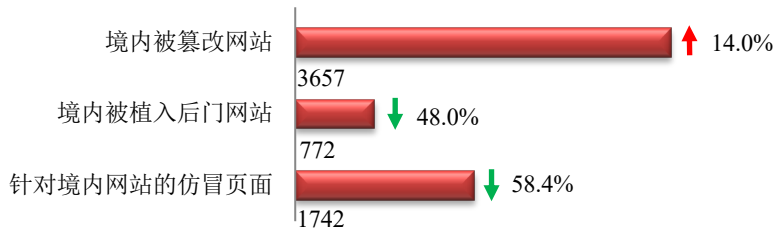
ANVA网络安全威胁信息共享平台

https://share.anva.org.cn/web/publicity/listurl

中国反网络病毒联盟（Anti Network-Virus Alliance of China，缩写 ANVA）是由 CNCERT 发起并组织运作的行业联盟。

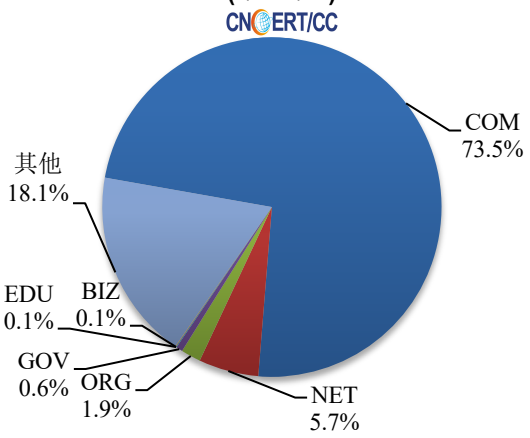
本周网站安全情况

本周 CNCERT 监测发现境内被篡改网站数量 3657 个；被植入后门的网站数量为 772 个；针对境内网站的仿冒页面数量为 1742 个。

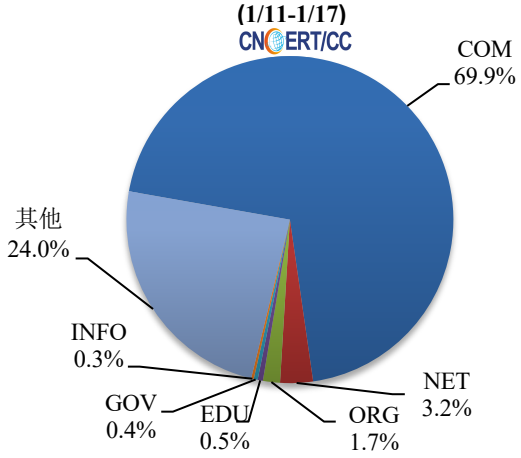


本周境内被篡改政府网站（GOV 类）数量为 23 个（约占境内 0.6%），较上周下降了 4.2%；境内被植入后门的政府网站（GOV 类）数量为 3 个（约占境内 0.4%），较上周下降了 86.4%。

本周我国境内篡改网站按类型分布
(1/11-1/17)

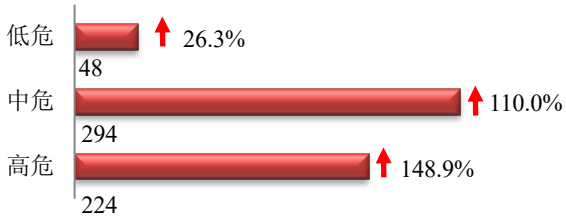


本周我国境内被植入后门网站按类型分布
(1/11-1/17)

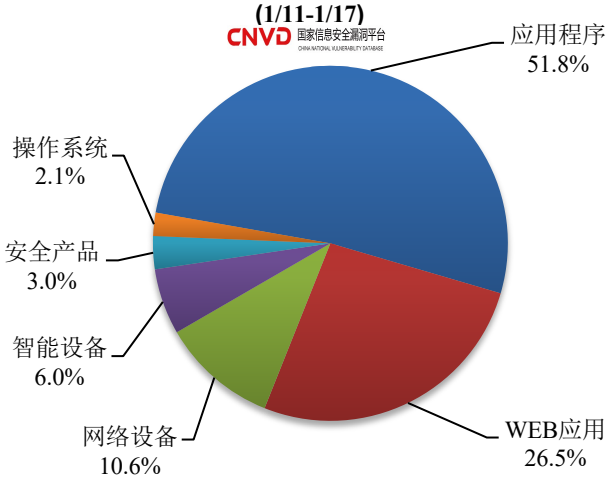


本周重要漏洞情况

本周，国家信息安全漏洞共享平台（CNVD）新收录网络安全漏洞 566 个，信息安全漏洞威胁整体评价级别为中。



本周CNVD收录漏洞按影响对象分布
(1/11-1/17)



本周 CNVD 发布的网络安全漏洞中，应用程序漏洞占比最高，其次是 WEB 应用和网络设备。

更多漏洞有关的详细情况，请见 CNVD 漏洞周报。

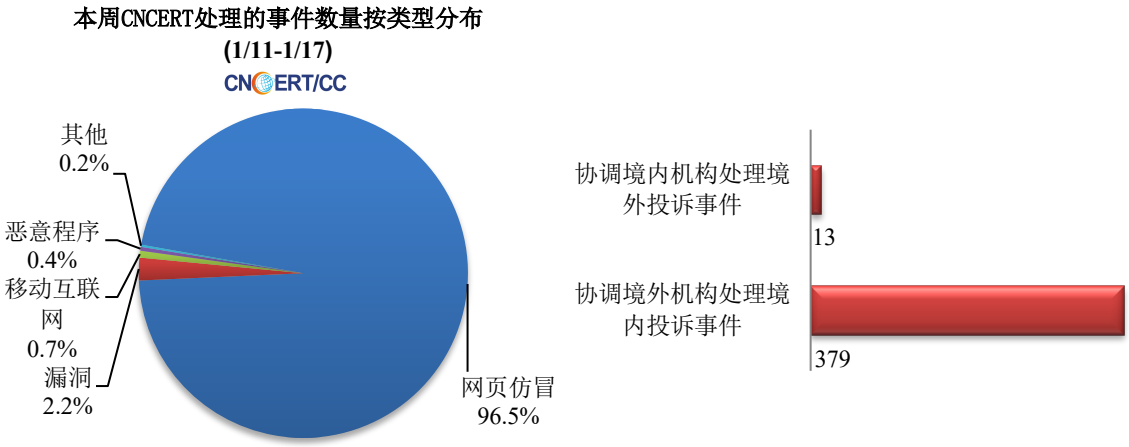
CNVD漏洞周报发布地址

http://www.cnvd.org.cn/webinfo/list?type=4

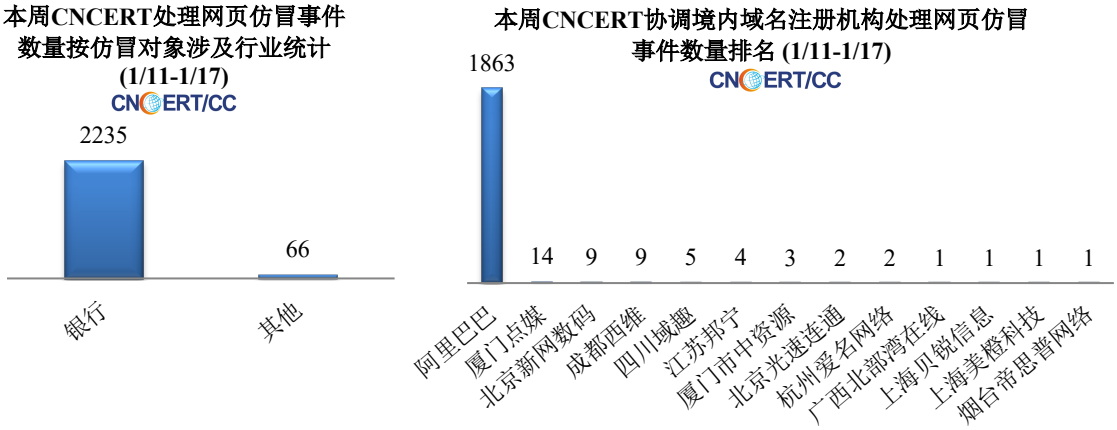
国家信息安全漏洞共享平台(缩写 CNVD)是 CNCERT 联合国内重要信息系统单位、基础电信企业、网络安全厂商、软件厂商和互联网企业建立的信息安全漏洞信息共享知识库。

本周事件处理情况

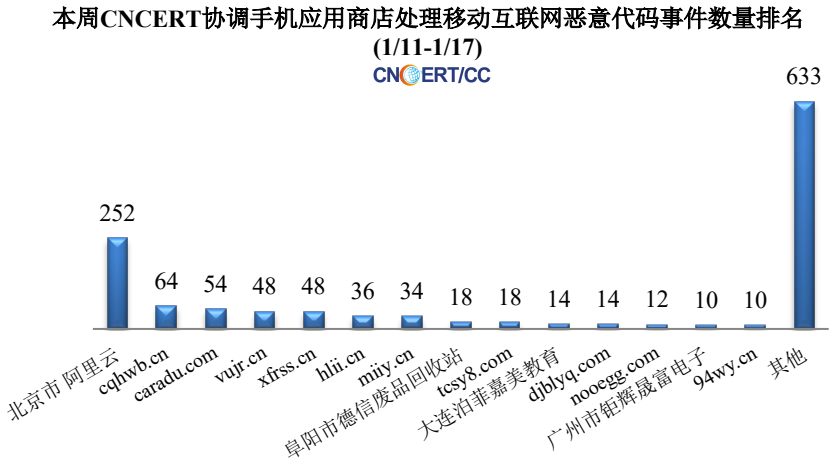
本周，CNCERT 协调基础电信企业、云服务商、域名注册服务机构、应用商店、各省分中心以及国际合作组织共处理了网络安全事件 2384 起，其中跨境网络安全事件 392 起。



本周，CNCERT 协调境内外域名注册机构、境外 CERT 等机构重点处理了 2301 起网页仿冒投诉事件。根据仿冒对象涉及行业划分，包括银行仿冒事件 2235 起以及其他事件 66 起。



本周，CNCERT 协调 286 个应用商店及挂载恶意程序的域名开展移动互联网恶意代码处理工作，共处理传播移动互联网恶意代码的恶意 URL 链接 1265 个。



业界新闻速递

1. 工业互联网企业网络安全分类分级管理试点工作启动

1 月 13 日，据工业和信息化部官网消息，工业和信息化部印发《关于开展工业互联网企业网络安全分类分级管理试点工作的通知》（以下简称《通知》），部署开展工业互联网企业网络安全分类分级管理试点工作。初定在天津、吉林、上海、江苏、浙江、安徽、福建、山东、河南、湖南、广东、广西、重庆、四川、新疆 15 个省（区、市）开展试点。

《通知》显示，本次试点的目的是通过试点，将进一步提升工业互联网企业网络安全分类分级规则标准、定级流程以及工业互联网安全系列防护规范的科学性、有效性和可操作性，加快构建工业互联网企业网络安全分类分级管理制度；进一步落实试点企业网络安全主体责任，形成可复制可推广的工业互联网网络安全分类分级管理模式；总结一批工业互联网网络安全典型解决方案，选拔一批优秀示范企业，培育一批专业服务机构。

《通知》要求，试点组织单位于 2021 年 2 月底前开展自主定级，完成定级报告。试点组织单位组织第三方专业机构对试点企业自主定级情况进行核查，于 2021 年 3 月底前指导试点企业完成定级核查。试点组织单位组织第三方专业机构，结合工业互联网企业网络安全分类分级防护系列规范，指导试点企业于 2021 年 9 月底前落实与自身等级相适应的安全防护措施。

2. 全国“断卡”行动开展第二轮集中收网

1 月 15 日，据公安部官网消息，1 月 15 日 15 时，在国务院打击治理电信网络新型违法犯罪工作部际联席会议办公室统一指挥下，全国“断卡”行动开展第二次集中收网行动，北京、天津、广东、

浙江等 23 个省区市公安机关同步开展对“11.30”专案违法犯罪团伙的集中抓捕，严厉打击整治非法开办贩卖电话卡、银行卡等“两卡”违法犯罪。截至 15 日 20 时，各地共抓获违法犯罪嫌疑人 405 名，缴获电话卡、银行卡共计 4.3 万张。

据了解，自去年 10 月全国“断卡”行动部署开展以来，各地各部门高度重视，在部际联席会议机制框架下主动担当作为，集中力量、多措并举，重拳打击整治非法开办贩卖电话卡银行卡违法犯罪。截至目前共打掉涉“两卡”违法犯罪团伙 7816 个，抓获涉“两卡”犯罪嫌疑人 14.8 万名，公开惩戒涉“两卡”违法犯罪嫌疑人 5.7 万余名，累计治理行业网点、机构 8869 个，打击治理工作取得阶段性明显成效。

国务院联席办有关负责人表示，将保持对非法开办贩卖电话卡银行卡违法犯罪活动的打击整治力度，深入推进专项行动，强化侦查打击，集中破案攻坚，依法从严惩处不法分子。同时，强化部门协作配合，落实主体责任，严厉整治重点行业和地区，加强源头治理，坚决铲除滋生此类违法犯罪土壤，切实维护人民群众合法权益和社会稳定。

关于国家互联网应急中心（CNCERT）

国家计算机网络应急技术处理协调中心（英文简称 CNCERT/CC），成立于 2001 年 8 月，为非政府非盈利的网络安全技术中心，是中国计算机网络应急处理体系中的牵头单位。作为国家级应急中心，CNCERT/CC 的主要职责是：按照“积极预防、及时发现、快速响应、力保恢复”的方针，开展互联网网络安全事件的预防、发现、预警和协调处置等工作，运行和管理国家信息安全漏洞共享平台（CNVD），维护公共互联网安全，保障关键信息基础设施的安全运行。

CNCERT/CC 在中国大陆 31 个省、自治区、直辖市设有分支机构，并通过组织网络安全企业、学校、社会组织和研究机构，协调骨干网络运营单位、域名服务机构和其他应急组织等，构建中国互联网安全应急体系，共同处理各类互联网重大网络安全事件。CNCERT/CC 积极发挥行业联动合力，发起成立了中国反网络病毒联盟（ANVA）和中国互联网网络安全威胁治理联盟（CCTGA）。

同时，CNCERT/CC 积极开展网络安全国际合作，致力于构建跨境网络安全事件的快速响应和协调处置机制。截至 2019 年，已与 78 个国家和地区的 260 个组织建立了“CNCERT/CC 国际合作伙伴”关系。CNCERT/CC 是国际应急响应与安全组织 FIRST 的正式成员，以及亚太计算机应急组织 APCERT 的发起者之一，还积极参加亚太经合组织、国际电联、上合组织、东盟、金砖等政府层面国际和区域组织的网络安全相关工作。

联系我们

如果您对 CNCERT《网络安全信息与动态周报》有何意见或建议，欢迎与我们的编辑交流。

本期编辑：马莉雅

网址：www.cert.org.cn

email：cncert_report@cert.org.cn

电话：010-82990315